09/945,172

DP
6/16/06

In the Specification

Please replace the title at page 1, line 1, with the following rewritten title:

SYSTEM AND METHOD FOR THE DETECTION OF AND REACTION TO ~~COMPUTER HACKER~~ DENIAL OF SERVICE ATTACKS

Please replace the title on the Abstract page 57, line 1, with the following rewritten title. A replacement sheet for the Abstract page is appended hereto.

SYSTEM AND METHOD FOR THE DETECTION OF AND REACTION TO ~~COMPUTER HACKER~~ DENIAL OF SERVICE ATTACKS

Please replace the paragraph beginning at page ~~15~~ 13, line 11, with the following rewritten paragraph:

MJD
6/15/06

-- The current best procedure for defending against such attacks, as documented in the CERT web site, consists of owners of web sites monitoring the network and server equipment they own for conditions of abnormally high utilization. When detected, high utilization is reported to the Internet Service Providers (ISPs) through which the

organization connects to the Internet. Each ISP network connects to a large number of organizations. The ISPs then search their networks in order to find areas of low utilization. The ISPs trace (i.e., record) all user traffic in that area of low utilization, and then scan the recorded traces looking for devices that are issuing sequences of commands of type and frequency that attacking zombies would issue. Zombies are easier to locate in areas of lower as opposed to higher utilization because the zombies contribute a relatively higher proportion of the records in the trace log, so their activity is more readily identified. Once a zombie is located, the ISP can trace all traffic from that zombie to the attacked system, thereby enabling those fighting the attack to better understand its nature. And although commands from the master computers to the zombies are not necessary once an attack has started, an ongoing trace of the zombie's activity can, with luck, record commands being sent from the zombie's master (the computer which has loaded attack code scripts into the zombie and activated the attack). When a master is found, it is possible not only to regain control of the master, but also to reclaim all of the zombies under its control. With very good luck, it may also be possible to take traces from a master computer and locate the hacker controlling the

master, although skilled hackers usually perform "hit and run" operations in which they start and stop attacks and erase their footprints in a matter of hours, long before the currently available problem diagnosis and identification processes can be effectively employed . ~~"Mafiaboy," a~~ A sixteen year old Canadian boy who brought down the sites of Amazon.com, Yahoo, e-Bay, and Charles Schwab, was identified months after his attacks not as a result of the extensive forensic diagnostic effort undertaken in response, but rather because the youth bragged in an online chat group (Ellen Messmer and Denise Pappalardo, *Network World*, Feb. 12, 2001).--.